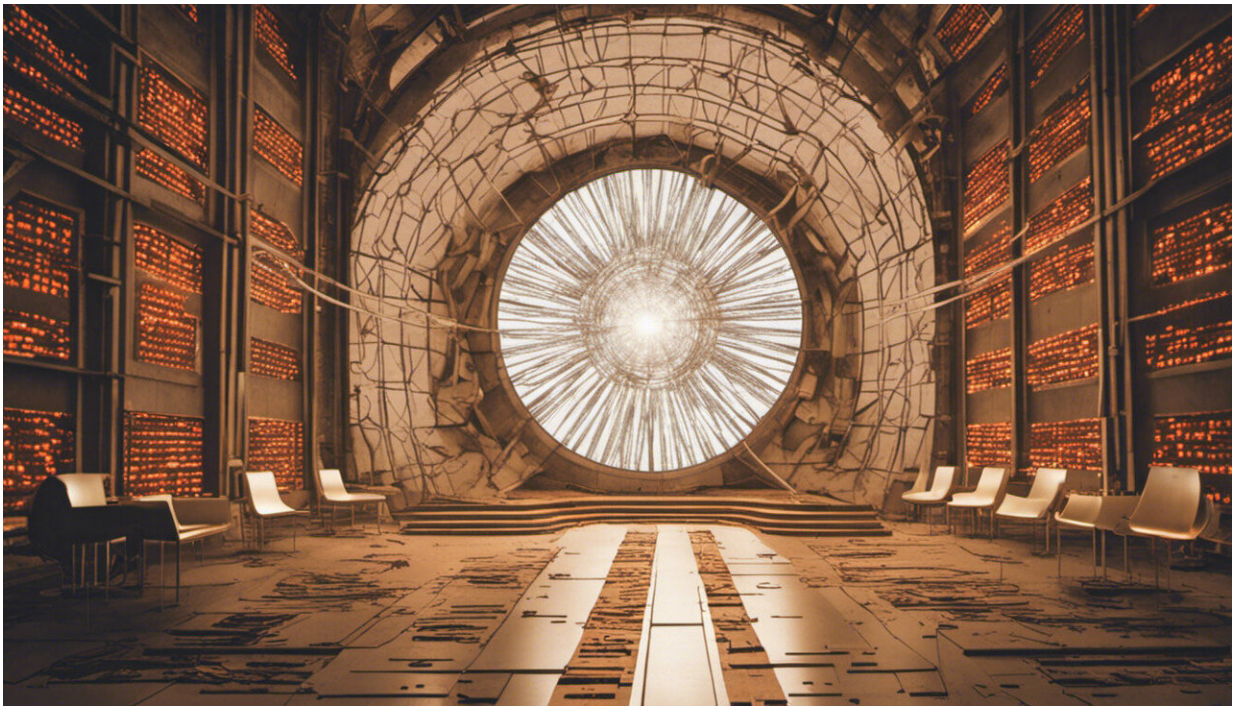
The argument from cyberspace for eliminating nuclear weapons

November 8 2018, by Lauren J. Borja And Mv Ramana



Credit: AI-generated image (disclaimer)

At the height of the Cold War in 1982, American psychiatrist Robert Jay Lifton argued that the "central existential fact of the nuclear age is vulnerability." That warning predated the proliferation of computers into almost every aspect of modern life, including nuclear weapons.

Today, the destructiveness of nuclear weapons has been coupled with the vulnerability of computers to create new pathways to disaster.

Specifically, there is now the possibility that hackers could compromise the computers that control nuclear weapons or provide information to officials about impending nuclear attacks.

Weapons security critically flawed

An October 2018 report reinforced this sense of vulnerability. In it, the United States Government Accountability Office (GAO) described a number of problems commonly found in the modern weapons systems developed by the U.S. Department of Defense (DOD). Although the report itself doesn't say so, officials confirmed that nuclear weapons programs were included in the study.

The findings of the GAO report echoed earlier warnings of the cyberthreat to nuclear weapons. These included a 2013 DOD report and one by the Nuclear Threat Initiative, a non-governmental nuclear weapon threat reduction organization based in Washington, D.C.

Our research examines the risks associated with nuclear weapons systems, including those of accidental or inadvertent nuclear war. The most pressing concern from the GAO report is the possibility that some of these vulnerabilities might affect "nuclear command and control," the term used to describe the computer networks that continuously monitor and direct the vast U.S. nuclear arsenal (or Russia).

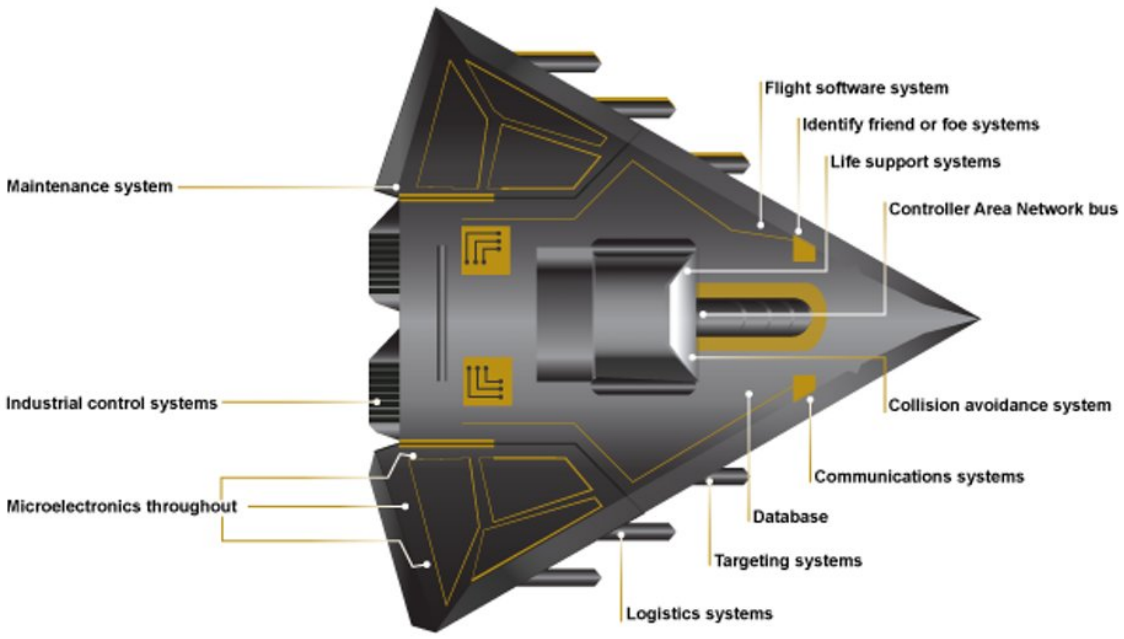
The recent GAO report broadly criticized all DOD weapons systems. Over the past five years (2012 to 2017), the GAO reported, "DOD testers routinely found mission-critical cyber-vulnerabilities in nearly all weapon systems that were under development. Using relatively simple tools and techniques, testers were able to take control of these systems

and largely operate undetected."

In other words, just about every weapon system being developed by the U.S. military is vulnerable to cyberattack. What stands out are both the scale of the problem and that these problems exist in systems that should be highly protected.

The computerized military

Computers play an outsized role in the U.S. military—from providing information through various sensors to forming the backbone of communications networks. Faster communications and increased access to information are both valuable assets and these goals can be achieved with computers. Computers have become ubiquitous in the military environment as countries demand quick access to information and communications.



Source: GAO analysis of Department of Defense information. | GAO-19-128

A graphic from the GAO report illustrating many of the potential computer systems built into modern weapons systems that could be vulnerable to hackers. Credit: U.S. Government Accountability Office

But computers also introduce vulnerabilities. As their role grows to include connecting the weapons systems of most advanced countries, so does our vulnerability. The vulnerability of these weapons systems should be seen as an anticipated and, arguably unavoidable, consequence of the computer-filled world we live in.

The GAO report went farther than just identifying vulnerabilities —it identified a culture within the DOD that fails to recognize and adequately address cybersecurity problems. Officials routinely assumed their systems were safe and ignored warnings until very recently.

We have observed a similar overconfidence in the military officials responsible for nuclear command and control.

This is a problem because the command-and-control system relies on complex networks of interconnected computers. These computers connect early warning satellites and radars to the president and will be used to pass on presidential orders to launch nuclear weapons should that fateful decision ever be made.

Computers must also constantly monitor and coordinate the daily operation of U.S. nuclear arsenal. Timelines for decisions in this system are extremely compressed, allowing less than 10 minutes for critical launch decisions to be made. The combination of interactive complexity and the tight timeline is typical of many other technological systems that are susceptible to unpredictable, large-scale accidents.

Computer errors that almost started nuclear wars

Unclassified reports reveal that problems within the computers of nuclear command and control date back to at least the 1970s, when a deficient computer chip signalled that 200 Soviet missiles were headed towards the U.S. Computer problems have persisted: In 2010, a loose circuit card caused a U.S. launch control centre to lose contact with 50 nuclear missiles. In both cases, the accident might have been mistaken for a deliberate attack. Failing to recognize the mistake could have resulted in the U.S. launching nuclear weapons.

These cases were presumably the result of unintentional errors, not deliberate actions. But hacking and other forms of targeted cyberattacks greatly increase the risk of accidental nuclear launch or other devastating actions. Overconfidence on the part of the officials overseeing the nuclear arsenal is therefore negligent and dangerous.

A more recent compounding factor is the ongoing, roughly trillion-dollar upgrade of the U.S. nuclear arsenal started by the Obama administration. This so-called modernization effort included upgrades to the nuclear command and control system. The Trump administration continues to make this a priority.

Modernization increases the possibility that changes to the nuclear command and control system will introduce new or reveal hitherto unknown vulnerabilities into the system. The evidence from the GAO report and other publicly available documents indicates that the officials in charge will be emphasizing speed, convenience, or cost over cybersecurity.

In its conclusion, the GAO report explained that the DOD "has taken several major steps to improve weapon systems cybersecurity." But the DOD "faces barriers that may limit its ability to achieve desired

improvements," such as constraints on information sharing and workforce shortages. That is not reassuring.

There is a more basic problem that we have emphasized above: the risks associated with cyberattacks can be ameliorated but not fully eliminated. When this intrinsic risk is integrated with the sheer destructiveness of nuclear weapons, the only way to avoid a catastrophic accident at some point in time is to embrace efforts to abolish the weapons themselves.

Provided by The Conversation